

REMARKS

By the present Amendment, Applicants have amended claims 1-7, 11 and 15-22 to further clarify the invention. Claims 1-22 remain pending in the present application.

The foregoing minor amendments are being filed in order to improve the clarity of the allowed claims, and accordingly, consideration and entry of the amendments is respectfully requested. Applicants submit that these minor amendments do not change the scope of or affect the allowability of the claims. These minor claim amendments are fully supported in Applicants specification and drawings. For example, in Fig. 1, in the "Addition" blocks of 107 and 110, a "point mP " and a "point $(m+1)P$ " are added (see also, pg. 19, lines 24-25, and pg. 20, lines 11-12). Further, as supported in Fig. 1, 106-108, 110 and 111, the "bit value" is the i -th bit of scalar value 106. The addition and doubling calculations represent the calculation groups of 107 and 108 and the calculation groups of 110 and 111. Applicants are submitting the above claim amendments for further clarification and respectfully request entry and allowance of these amendments.

To the extent necessary, Applicant petitions for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees and excess claim fees, to Deposit Account No. 50-1417 (referencing case No. 500.39908X00) and please credit any excess fees to such deposit account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 684-1120